Marktconsultatie

Europese aanbesteding

Managed Private Cloud

Auteur: De heer A. Harbers (Pro Mereor) en mevrouw A. Ruiters van Eijden (Regionale ICT-Dienst Utrecht)

Datum: 12 januari 2026

Inhoudsopgave

Definities

In dit document wordt een aantal begrippen gebruikt. Begrippen worden met een hoofdletter geschreven. Gedefinieerde begrippen kunnen zowel in enkelvoud als in meervoud worden gebruikt.

Begrip	**Definitie**
Aanbestedende dienst	Regionale ICT-dienst Utrecht.
Deelnemer	Marktpartij die deelneemt aan deze Marktconsultatie.
Marktconsultatie	Een informatie-uitwisseling tussen een Aanbestedende dienst en marktpartijen om marktpartijen te raadplegen over een eventuele of voorgenomen Aanbesteding.

1 Inleiding

In deze analyse zijn de ontvangen antwoorden van Deelnemers verwerkt en per vraag zijn waar mogelijk kort en bondig de overeenkomsten en verschillen geduid en een conclusie geformuleerd.

2 Analyse antwoorden op vragen

Analyse antwoorden op vraag 1
Beschrijf de onderneming in max. 100 woorden.

Overeenkomsten

- Alle deelnemers beschrijven zichzelf als ervaren IT-dienstverleners met een sterke focus op cloud-oplossingen, security en de publieke sector.
- Er wordt brede ervaring met managed services en infrastructurele projecten voor (semi-)overheidsinstellingen gerapporteerd.
- Deelnemers benadrukken hun lokale aanwezigheid in Nederland en hun kennis van de specifieke Nederlandse wet- en regelgeving.

Verschillen

- Deelnemer 1 en 3 benadrukken hun nationale of internationale schaal en eigen infrastructuurbasis.
- Deelnemer 2 focust specifiek op de combinatie van software-oplossingen, data en cloud.
- Deelnemer 5 profileert zich expliciet als een volledig Nederlandse cloud-native specialist.

Conclusie
De markt bestaat uit volwassen Deelnemers die allen claimen over de juiste expertise en ervaring te beschikken om de Aanbestedende dienst te ondersteunen bij een managed private cloud transitie.

Analyse antwoorden op vraag 2
Hoe zou u de markt van de virtuele datacenters omschrijven?

Overeenkomsten

- De markt wordt door alle Deelnemers omschreven als zeer volwassen, stabiel en technisch uitgekristalliseerd. De basistechnologie (veelal VMware) is bij de meeste Deelnemers identiek.
- Er is een duidelijke trend waarneembaar naar soevereine cloud-oplossingen. Organisaties binnen de overheid kiezen vaker voor private cloud vanwege strikte wet- en regelgeving (zoals NIS2 en de BIO) en de wens om data binnen de landsgrenzen te houden.
- Private cloud wordt niet langer gezien als een tussenstap naar de public cloud, maar als een permanent en essentieel onderdeel van een hybride cloud-strategie voor kritieke workloads.
- De markt is zeer competitief, wat resulteert in een breed aanbod van kwalitatief gelijkwaardige infrastructurele diensten.

Verschillen

- Sommige deelnemers wijzen op een sterke consolidatieslag waarbij alleen grotere spelers kunnen blijven investeren in de benodigde security- en compliance-certificeringen.
- Andere deelnemers zien juist een herwaardering van gespecialiseerde, lokale aanbieders die meer flexibiliteit en nabijheid bieden dan de grote internationale Deelnemers.
- Er is een verschil in visie op de rol van de leverancier: waar de een de markt typeert als een pure infrastructuurmarkt, ziet de ander een verschuiving naar een regiemarkt waarbij de leverancier **optreedt** als integrator van verschillende cloudomgevingen.

Conclusie
De markt is volwassen en biedt de Aanbestedende dienst voldoende keuze uit gekwalificeerde marktpartijen. Omdat de technische basis bij de meeste deelnemers vergelijkbaar is, zit het

onderscheid voor de Aanbestedende dienst vooral in de 'schil' rondom de techniek: de kwaliteit van de beheerorganisatie, de mate van soevereiniteit, de geboden flexibiliteit in de samenwerking en de ondersteuning bij compliancevraagstukken.

Analyse antwoorden op vraag 3
Welke trends en ontwikkelingen verwacht u op het gebied van de gevraagde dienstverlening in de komende vijf jaar?

Overeenkomsten

- De markt voorziet een sterke toename in de focus op digitale soevereiniteit en gegevensbescherming. Organisaties willen volledige controle over waar hun data staat en wie er toegang toe heeft, mede gedreven door strengere Europese wet- en regelgeving.
- Er wordt een breed gedragen verschuiving verwacht naar AI-gestuurd beheer (AIOps). Hierbij wordt kunstmatige intelligentie ingezet om verstoringen te voorspellen, beheerprocessen te automatiseren en de algehele efficiëntie van de cloudomgeving te verhogen.
- Cybersecurity blijft een topprioriteit, waarbij de nadruk verschuift van reactieve beveiliging naar een 'zero trust' architectuur en continue monitoring om te voldoen aan richtlijnen zoals NIS2 en DORA.
- Duurzaamheid en energie-efficiëntie van datacenters (Green IT) worden integrale onderdelen van de dienstverlening, mede door de rapportageverplichtingen vanuit de CSRD.

Verschillen

- Deelnemer 3 en 6 leggen een specifieke nadruk op de opkomst van FinOps, waarbij de focus ligt op het beheersen en optimaliseren van de variabele kosten binnen een hybride cloudmodel.
- Deelnemer 9 verwacht dat technologische abstractielagen (zoals containerisatie en serverless) ervoor zorgen dat de fysieke infrastructuur nog verder naar de achtergrond verdwijnt, terwijl andere deelnemers juist het belang van dedicated hardware voor specifieke workloads blijven benadrukken.
- Deelnemer 1 en 4 zien een trend naar verdere consolidatie van diensten bij enkele grote platformleveranciers, terwijl Deelnemer 5 en 7 juist een groeiende behoefte zien aan een 'multi-cloud' benadering om afhankelijkheid van één leverancier (vendor lock-in) te voorkomen.

Conclusie
De komende vijf jaar staan in het teken van de transformatie van 'pure infrastructuur' naar een 'intelligent en soeverein platform'. De Aanbestedende dienst doet er goed aan om in de aanbesteding niet alleen te sturen op de techniek van vandaag, maar ook op het vermogen van de leverancier om mee te bewegen met AI-innovaties, strikte compliance-eisen en duurzaamheidsdoelstellingen. Een flexibele contractvorm die innovatie stimuleert in plaats van beperkt, is hierbij essentieel.

Analyse antwoorden op vraag 4
In welke opzichten verwachten jullie zich te kunnen onderscheiden van andere marktpartijen?

Overeenkomsten

- Deelnemers benadrukken unaniem hun diepgaande kennis van de Nederlandse (semi-)overheidsmarkt en de specifieke eisen die daar worden gesteld, zoals de BIO en de overgang naar NIS2.
- Er wordt sterk ingezet op lokale nabijheid en persoonlijke aandacht. Men onderscheidt zich door korte communicatielijnen, vaste contactpersonen (zoals Service Delivery Managers) en een partnership-benadering in plaats van een puur leverancier-klantmodel.
- Alle partijen profileren zich op het gebied van hoogwaardige security en compliance, waarbij zij beschikken over de relevante certificeringen (ISO 27001, NEN 7510, ISAE 3402) om de Aanbestedende dienst volledig te ontzorgen op audit-vlak.

Verschillen

- Deelnemer 4 en 9 onderscheiden zich door hun enorme schaal en internationale 'backbone', waardoor zij toegang hebben tot wereldwijde innovaties en zeer grote investeringskracht.
- Deelnemer 1 en 5 leggen de nadruk op hun onafhankelijke positie als 100% Nederlandse partij, waarbij zij soevereiniteit als hun belangrijkste wapenfeit zien tegenover internationale grootmachten.
- Deelnemer 7 profileert zich specifiek door een breed 'ecosysteem' aan te bieden, waarbij niet alleen de infrastructuur maar ook de bovenliggende applicatie- en werkpleklaag naadloos kunnen worden geïntegreerd.
- Deelnemer 8 zet in op een 'cloud-agnostische' benadering, waarbij zij zich onderscheiden door de vrijheid die zij de klant bieden om workloads eenvoudig te verplaatsen zonder vendor lock-in.

Conclusie

De Aanbestedende dienst kan kiezen uit verschillende smaken van onderscheidend vermogen. De keuze ligt tussen de 'veilige haven' van grote internationale Deelnemers met veel schaalvoordeel, versus de 'wendbare partners' die volledig Nederlands zijn en dichter op de operatie staan. Voor de Aanbestedende dienst is het van belang om te bepalen of het accent moet liggen op technische schaalbaarheid of op de flexibiliteit en nabijheid van de beheerorganisatie.

Analyse antwoorden op vraag 5

Op welke wijze zijn jullie autonoom en wordt de autonomie gegarandeerd t.o.v. mogendheden buiten de EER?

Overeenkomsten

- Alle deelnemers verklaren dat zij uitsluitend gebruikmaken van datacenters die fysiek op Nederlands grondgebied (of binnen de EER) staan. Hiermee wordt gegarandeerd dat alle data onder de Nederlandse wetgeving en de AVG valt.
- De meerderheid van de Deelnemers geeft aan dat zij werken met lokaal personeel (Nederlandssprekend en woonachtig in de EER) dat gescreend is (bijv. VOG of een veiligheidsonderzoek).
- Er is brede consensus over het feit dat er geen data wordt gedeeld met moederbedrijven of autoriteiten buiten de EER, tenzij er een wettelijke verplichting is die door een Nederlandse rechter wordt bekrachtigd.
- Certificeringen zoals ISO 27001 en NEN 7510 worden door alle Deelnemers aangehaald als bewijs voor hun robuuste informatiebeveiliging en beheersing van externe risico's.

Verschillen

- Deelnemer 1, 4 en 9 (de grotere internationale Deelnemers) wijzen op hun juridische structuren die hen beschermen tegen wetgeving zoals de Amerikaanse Cloud Act, maar erkennen dat zij onderdeel zijn van een groter internationaal concern.
- Deelnemer 5 en 8 onderscheiden zich expliciet door te stellen dat zij 100% Nederlands eigendom zijn. Zij voeren aan dat zij hiermee elk risico op extraterritoriale wetgeving (zoals de Cloud Act) fundamenteel uitsluiten, omdat er geen enkele juridische band is met mogendheden buiten de EER.
- Deelnemer 7 benadrukt de mogelijkheid van "air-gapped" beheer, waarbij beheerverbindingen fysiek gescheiden zijn van het internet om elke vorm van ongeautoriseerde toegang van buitenaf te blokkeren.
- Enkele deelnemers focussen meer op de technologische autonomie door het gebruik van open-source standaarden om afhankelijkheid van specifieke Amerikaanse softwareleveranciers (vendor lock-in) te minimaliseren.

Conclusie

Voor de Aanbestedende dienst is het essentieel om te bepalen welk niveau van autonomie vereist is. Hoewel alle Deelnemers voldoen aan de basisregels van dataopslag in Nederland, bieden de puur Nederlandse Deelnemers een hogere mate van juridische bescherming tegen invloeden van buiten de EER. Indien de Aanbestedende dienst maximale soevereiniteit wenst, is de eigendomsstructuur van de leverancier een kritiek selectiecriterium. Daarnaast is de screening van beheerpersoneel en de fysieke locatie van de beheerorganisatie een belangrijk punt om contractueel te borgen.

Analyse antwoorden op vraag 6

Verwacht u alle werkzaamheden m.b.t. de gevraagde producten en dienstverlening in eigen beheer uit te kunnen voeren of zou u voor deze opdracht werken met onderaannemers of in combinatie (derden) inschrijven?

Overeenkomsten

- Vrijwel alle Deelnemers geven aan de kern van de dienstverlening – het technisch beheer van de private cloud en de dagelijkse operatie – volledig in eigen beheer uit te voeren met eigen personeel.
- Er is consensus dat voor facilitaire zaken, zoals de fysieke datacenterlocatie (indien niet in eigen bezit), gebruik wordt gemaakt van gespecialiseerde Nederlandse colocatie-partners.
- Bijna alle deelnemers maken gebruik van externe leveranciers voor hardware-onderhoud (ondersteuning door fabrikanten) en voor de levering van licenties.
- De verantwoordelijkheid en regie over de gehele keten blijven bij alle Deelnemers in eigen beheer liggen, waarbij zij optreden als het centrale aanspreekpunt (hoofdaannemer) voor de Aanbestedende dienst.

Verschillen

- Deelnemer 4 en 9 geven aan dat zij voor zeer specialistische werkzaamheden (zoals complexe security-audits of niche-consultancy) gebruik kunnen maken van vaste partners binnen hun internationale concern.
- Deelnemer 7 en 8 benadrukken expliciet dat zij indien nodig in een 'combinatie' of ecosysteem-model kunnen inschrijven om een full-stack oplossing (inclusief applicatiebeheer) te bieden, terwijl anderen strikt vasthouden aan eigen uitvoering voor de volledige scope.

- Deelnemer 1 geeft aan dat bepaalde logistieke processen rondom hardware-vervanging gestandaardiseerd zijn uitbesteed aan partners, terwijl Deelnemer 3 dit juist als een eigen kernactiviteit beschouwt.

Conclusie
De markt is prima in staat om de gevraagde diensten te leveren, waarbij de regie stevig in handen van de hoofdaannemer blijft. Voor de Aanbestedende dienst betekent dit dat de continuïteit van de dienstverlening niet afhankelijk is van een complexe keten van onderaannemers. Het is echter raadzaam om in de definitieve uitvraag te eisen dat alle beheeractiviteiten vanuit de EER worden uitgevoerd en dat de leverancier transparant is over welke specifieke rollen (zoals datacenter-faciliteiten of specialistische security) door derden worden ingevuld.

Analyse antwoorden op vraag 7
Indien u met derden inschrijft, welk deel van de opdracht overweegt u dan aan hen uit te besteden?

Overeenkomsten
- Deelnemers geven aan dat de kern van de dienstverlening (beheer en regie) vrijwel altijd in eigen beheer blijft. Derden worden uitsluitend overwogen voor ondersteunende of zeer specialistische deeltaken.
- Voor de fysieke datacenterfaciliteiten (stroom, koeling, fysieke beveiliging) maken bijna alle Deelnemers gebruik van gespecialiseerde colocatie-partners indien zij niet over eigen datacenters beschikken.
- Onderhoud en support op hardware (ondersteuning op locatie door de fabrikant) en de levering van softwarelicenties worden standaard bij derden (vendors) belegd.
- Specialistische security-diensten, zoals onafhankelijke penetratietesten of specifieke SOC-monitoring, worden door meerdere Deelnemers als een logisch onderdeel voor uitbesteding aan derden gezien.

Verschillen
- Deelnemer 4 en 9 kunnen voor specifieke consultancy of complexe migratievraagstukken putten uit een internationaal netwerk van zusterbedrijven of vaste partners, terwijl kleinere Deelnemers hiervoor eerder lokale zzp-netwerken of niche-partijen inschakelen.
- Deelnemer 7 geeft aan dat zij bij een zeer brede uitvraag (bijvoorbeeld inclusief applicatiebeheer) een strategische partner kunnen betrekken om een integrale 'full-stack' oplossing te bieden.
- Deelnemer 5 en 8 benadrukken dat zij proberen de afhankelijkheid van derden voor de technische uitvoering tot een absoluut minimum te beperken om maximale controle en soevereiniteit te waarborgen.

Conclusie
De Aanbestedende dienst hoeft niet te vrees voor een versnipperde verantwoordelijkheid; de Deelnemers treden op als hoofdaannemer en houden de regie op de kritieke processen zelf in handen. De inzet van derden beperkt zich hoofdzakelijk tot de 'facilitaire laag' (het gebouw en de hardware-garantie) en specialistische 'audit-taken'. Voor de Aanbestedende dienst is het raadzaam om in de definitieve uitvraag te verzoeken om een transparant overzicht van deze ketenpartners, inclusief hun land van herkomst, om de eerder besproken autonomie te borgen.

Analyse antwoorden op vraag 8

De bestaande datacenters worden 1 juli 2027 beëindigd, voor die tijd moet de cloudmigratie gerealiseerd zijn. Is dit een haalbare planning? En zo ja, wat is volgens jullie de ideale startdatum voor het daadwerkelijke migratieproject?

Overeenkomsten

- Alle Deelnemers achten de deadline van 1 juli 2027 technisch haalbaar, mits er voldaan wordt aan een aantal strikte randvoorwaarden.
- Er is consensus dat een dergelijk traject een doorlooptijd van 12 tot 18 maanden vereist. Dit is inclusief de voorbereiding, de inrichting van de landingszone en de feitelijke migratie van workloads.
- De ideale startdatum voor het project ligt volgens de Deelnemers uiterlijk in het eerste kwartaal van 2026. Dit betekent dat de aanbesteding en de gunning uiterlijk eind 2025 afgerond moeten zijn.
- Deelnemers benadrukken dat een tijdige start essentieel is om voldoende ruimte te hebben voor onvoorziene vertragingen bij de migratie van complexe legacy-applicaties.

Verschillen

- Deelnemer 2 en 3 adviseren om niet te wachten op de volledige inrichting, maar direct te starten met een "wave-gebaseerde" aanpak waarbij eenvoudige applicaties al vroeg gemigreerd worden.
- Deelnemer 5 en 6 wijzen erop dat de planning staat of valt met de kwaliteit van de huidige documentatie van de Aanbestedende dienst. Als deze ontbreekt, moet de startdatum naar voren worden geschoven om eerst een "discovery-fase" uit te voeren.
- Deelnemer 9 merkt op dat de vakantieperiodes en de 'bevriezing' van systemen rond de jaarwisseling vaak onderschat worden in de planning en adviseert hier extra buffer voor op te nemen.
- Deelnemer 8 stelt dat de haalbaarheid ook afhangt van de beschikbare capaciteit bij de Aanbestedende dienst zelf voor het testen van de applicaties na migratie.

Conclusie

De markt geeft een duidelijk signaal: 1 juli 2027 is haalbaar, maar de tijd is krap. Om de risico's te minimaliseren, moet de Aanbestedende dienst uiterlijk in januari 2026 starten met de uitvoering. De belangrijkste succesfactor is een snelle afronding van het aanbestedingstraject in 2025. Het advies aan de Aanbestedende dienst is om nu al te starten met het actualiseren van de applicatie-inventarisatie en de afhankelijkheden (CMDB), zodat de winnende leverancier direct na gunning kan starten zonder een tijdrovende inventarisatieslag.

Analyse antwoorden op vraag 9

Kunt u aangeven of de door de RID ingeschatte opdrachtwaarde gelet op de scope realistisch is en zo niet waarom niet?

Overeenkomsten

- De meerderheid van de Deelnemers geeft aan dat de inschatting in de basis realistisch oogt, mits de scope beperkt blijft tot de kern van de gevraagde managed private clouddiensten.
- Er is consensus dat de werkelijke kosten sterk afhankelijk zijn van de uiteindelijke keuzes die de Aanbestedende dienst maakt op het gebied van autonomie (fysiek versus logisch gescheiden) en de gewenste diepgang van het beheer.

- Meerdere Deelnemers benadrukken dat de transitie- en migratiekosten vaak een aanzienlijk deel van de initiële opdrachtwaarde beslaan en dat deze niet onderschat mogen worden in de totale begroting.

Verschillen
- Deelnemer 2 en 4 plaatsen kanttekeningen bij de waarde indien er sprake is van een grote hoeveelheid legacy-systemen die intensief handmatig beheer vereisen; zij achten de waarde in dat geval aan de krappe kant.
- Deelnemer 9 merkt op dat indien specialistische security-diensten (zoals een volledig SOC/SIEM-koppeling en uitgebreide compliance-rapportages) integraal onderdeel worden, de opdrachtwaarde mogelijk naar boven bijgesteld moet worden.
- Deelnemer 5 en 8 geven aan dat de prijsstelling van softwarelicenties (met name de recente wijzigingen in de markt rondom VMware) een onzekere factor is die de haalbaarheid van de huidige opdrachtwaarde onder druk kan zetten.

Conclusie
De Aanbestedende dienst heeft met de huidige inschatting een realistisch vertrekpunt, maar moet rekening houden met een aantal 'prijsopdrijvende' factoren. Het advies is om in de aanbesteding een duidelijk onderscheid te maken tussen de eenmalige migratiekosten en de maandelijkse exploitatiekosten. Daarnaast is het essentieel om de keuzes rondom fysieke isolatie en de diepgang van specialistisch beheer (zoals databases) scherp te definiëren, aangezien deze factoren bepalend zijn voor het wel of niet passen binnen de geraamde opdrachtwaarde.

Analyse antwoorden op vraag 10
Welke risico's ziet u bij deze aanbesteding?

Overeenkomsten
- Deelnemers benoemen de krappe planning voor de datacenter-exit per 1 juli 2027 als een aanzienlijk risico. Vertraging in de aanbestedingsfase of bij de inrichting van de landingszone zet de migratie van workloads direct onder grote druk.
- Er is grote zorg over de kwaliteit en volledigheid van de huidige documentatie (CMDB) en de technische staat van de legacy-omgeving. Onduidelijkheid over afhankelijkheden tussen applicaties kan leiden tot onvoorziene complexiteit en vertraging tijdens de migratie.
- De schaarste aan gekwalificeerd personeel, zowel bij de leverancier als bij de Aanbestedende dienst, wordt als een risico gezien. Voor de transitie is specifieke kennis nodig die gedurende het hele project beschikbaar moet blijven.
- Het risico op een te rigide technische uitvraag wordt genoemd. Als de Aanbestedende dienst te gedetailleerd voorschrijft *hoe* de techniek moet worden ingericht, beperkt dit de innovatiekracht van Deelnemers en kan dit leiden tot onnodig hoge kosten.

Verschillen
- Deelnemer 2 en 5 wijzen specifiek op het risico van de recente wijzigingen in het licentiemodel van VMware (Broadcom), wat een onvoorspelbare impact kan hebben op de toekomstige exploitatiekosten.
- Deelnemer 8 benadrukt het risico van 'scope creep', waarbij gedurende het project extra eisen aan autonomie of beveiliging worden toegevoegd die niet in de oorspronkelijke businesscase waren opgenomen.

- Deelnemer 4 ziet een risico in de politieke besluitvorming binnen de deelnemende organisaties van de Aanbestedende dienst, wat kan leiden tot vertragingen in goedkeuringsprocessen tijdens de migratie.

Conclusie
Het beheersen van de planning en de informatievoorziening is cruciaal voor het succes van deze aanbesteding. De Aanbestedende dienst wordt geadviseerd om op korte termijn een 'discovery'-slag te maken op de huidige omgeving om de feitelijke migratie-effort scherp te krijgen. Daarnaast is het raadzaam om in de uitvraag ruimte te laten voor de expertise van de leverancier (functioneel specificeren) en een realistische risicoverdeling af te spreken, met name rondom factoren waar de leverancier geen invloed op heeft (zoals licentiewijzigingen van derden of interne besluitvorming).

Analyse antwoorden op vraag 11
Wat zou voor jullie een no-bid zijn voor deze aanbesteding?

Overeenkomsten
- Deelnemers geven unaniem aan dat een disbalans in de risicoverdeling een belangrijke reden is voor een no-bid. Dit betreft met name onredelijke of onbeperkte aansprakelijkheidseisen die niet in verhouding staan tot de opdrachtwaarde.
- Gunning op basis van 100% laagste prijs wordt door vrijwel alle Deelnemers als onwenselijk gezien. Men stelt dat bij kritieke infrastructuur kwaliteit, veiligheid en continuïteit de doorslag moeten geven.
- Een onrealistische planning, zoals een te korte transitieperiode zonder ruimte voor onvoorziene vertragingen, wordt als een groot risico beschouwd dat tot een no-bid kan leiden.
- Onduidelijkheid over de scope of de technische staat van de huidige omgeving (ontbreken van een betrouwbare CMDB) maakt het voor Deelnemers onmogelijk om een verantwoorde aanbieding te doen.

Verschillen
- Deelnemer 5 en 7 noemen specifiek de verplichte overname van personeel (OBO) als een breekpunt. Zij geven aan dat hun eigen organisatie- en beheerstructuur hier niet op is ingericht.
- Deelnemer 1 en 4 wijzen op zeer specifieke juridische clausules rondom intellectueel eigendom of extreme boeteclausules die niet marktconform zijn als mogelijke redenen om niet in te schrijven.
- Deelnemer 8 merkt op dat het eisen van een specifieke technologische oplossing (bijvoorbeeld een verplichting op één specifiek merk hardware) een no-bid kan zijn als zij hierdoor hun eigen standaardisatie en schaalvoordelen verliezen.
- Deelnemer 3 geeft aan dat het ontbreken van een reële dialoogmogelijkheid tijdens de aanbestedingsfase het risico voor hen te groot maakt.

Conclusie
Om voldoende kwalitatieve inschrijvingen te waarborgen, moet de Aanbestedende dienst zorgen voor marktconforme contractvoorwaarden. De belangrijkste factoren om een no-bid te voorkomen zijn: een evenwichtige aansprakelijkheidsregeling (maximaal 1x de jaarwaarde is gebruikelijk), een gunningsmodel waarbij kwaliteit zwaar weegt, en een transparante informatievoorziening over de huidige omgeving. Daarnaast wordt geadviseerd om terughoudend te zijn met eisen rondom

personeelsovername en om de technische invulling (het 'hoe') deels bij de expertise van de Deelnemers te laten.

Analyse antwoorden op vraag 12
Wat verwacht u van de opdrachtgever (RID) om de opdracht goed te kunnen uitvoeren?

Overeenkomsten

- Deelnemers verwachten een actuele en volledige inventarisatie van het huidige IT-landschap (CMDB), inclusief alle applicatie-afhankelijkheden, interfaces en technische vereisten. Dit is cruciaal voor een vlekkeloze transitie.
- Er wordt een actieve betrokkenheid van de Aanbestedende dienst gevraagd in de vorm van een gemandateerd projectteam en beschikbaarheid van applicatie-eigenaren en inhoudelijk deskundigen voor overleg en besluitvorming.
- Deelnemers benadrukken het belang van een duidelijke regie-organisatie aan de zijde van de Aanbestedende dienst die de interface vormt tussen de verschillende deelnemende gemeenten/organisaties en de Deelnemer.
- Er wordt verwacht dat de Aanbestedende dienst zorgdraagt voor tijdige acceptatietesten van de gemigreerde workloads, aangezien de Deelnemer de werking van de applicatie zelf vaak niet tot in detail kan beoordelen.
- Transparante communicatie en een partnership-mentaliteit worden essentieel geacht om gezamenlijk de strakke deadline van 2027 te halen.

Verschillen

- Deelnemer 1 en 5 vragen specifiek om een duidelijke visie op de gewenste mate van autonomie en security-eisen aan het begin van het traject, om kostbare wijzigingen achteraf te voorkomen.
- Deelnemer 3 en 8 wijzen op de noodzaak dat de Aanbestedende dienst verantwoordelijk blijft voor de communicatie naar de eigen interne eindgebruikers over de impact en de planning van de migratie.
- Deelnemer 9 verwacht dat de Aanbestedende dienst actief meewerkt aan het standaardiseren van processen (zoals change management) om de efficiëntie van de managed services te kunnen garanderen.
- Deelnemer 4 merkt op dat de Aanbestedende dienst tijdig moet zorgen voor de benodigde connectiviteit (bijvoorbeeld glasvezelverbindingen) tussen de eigen locaties en de datacenters van de Deelnemer

Conclusie
Een succesvolle uitvoering van de opdracht is geen eenzijdige verantwoordelijkheid van de Deelnemer. De markt vraagt van de Aanbestedende dienst een hoge mate van "volwassenheid als opdrachtgever". Dit betekent concreet: zorg dat de data over de huidige omgeving op orde is, richt een sterke centrale regie-organisatie in en wees bereid om snel besluiten te nemen. De Aanbestedende dienst fungeert als de onmisbare schakel tussen de functionele behoeften van de gemeenten en de technische uitvoering door de Deelnemer.

Analyse antwoorden op vraag 13
Hebben jullie vergelijkbare trajecten doorlopen. Kunnen jullie zich vinden in deze aanpak en/of ziet u hier kanttekeningen bij (zaken om rekening mee te houden)?

Overeenkomsten

- Alle Deelnemers bevestigen ruime ervaring te hebben met vergelijkbare grootschalige cloudtransities en datacenter-exits, specifiek binnen de publieke sector en bij samenwerkingsverbanden van gemeenten.
- Er is brede instemming met de voorgestelde gefaseerde aanpak. Deelnemers herkennen de noodzaak van een gedegen voorbereiding (fase 1 en 2) voordat de daadwerkelijke migratie start.
- De markt onderstreept unaniem dat het succes van een dergelijk traject valt of staat met de kwaliteit van de 'landingszone' (de technische inrichting van de nieuwe omgeving) en een bewezen migratiemethodiek.
- Alle Deelnemers waarschuwen voor de onderschatte complexiteit van legacy-applicaties en de noodzaak om per applicatie de juiste migratiestrategie (bijv. rehost, replatform of retire) te bepalen.

Verschillen
- Deelnemer 2 en 5 plaatsen een kanttekening bij de 'big bang' benadering; zij adviseren een meer iteratieve aanpak waarbij per 'wave' van applicaties wordt geleerd en bijgestuurd.
- Deelnemer 8 en 9 wijzen erop dat de aanpak momenteel sterk technisch georiënteerd lijkt. Zij adviseren om meer aandacht te besteden aan de organisatorische verandering bij de Aanbestedende dienst (adoptie en nieuwe manier van werken).
- Enkele Deelnemers adviseren om een 'exitstrategie' vanaf het begin integraal onderdeel te maken van de aanpak, om toekomstige vendor lock-in te voorkomen.
- Deelnemer 4 merkt op dat de aanpak rekening moet houden met de specifieke eisen van externe applicatieleveranciers van de Aanbestedende dienst, die vaak eigen voorwaarden stellen aan de infrastructuur waar hun software op draait.

Conclusie
De Aanbestedende dienst hanteert een aanpak die door de markt als professioneel en herkenbaar wordt beoordeeld. De belangrijkste aanbeveling is om de aanpak aan te vullen met een sterke focus op de 'zachte' kant van de transitie (organisatie en adoptie) en de regie op externe softwareleveranciers. Het advies is om in de uitvraag te vragen naar de specifieke migratiemethodiek van de Deelnemer en hoe zij omgaan met onvoorziene technische schuld in de legacy-omgeving.

Analyse antwoorden op vraag 14
Welke kosten- en verrekenmodellen hanteren jullie?

Overeenkomsten
- Alle Deelnemers hanteren een model dat gebaseerd is op een combinatie van eenmalige kosten (transitie/migratie) en maandelijkse operationele kosten (exploitatielasten).
- Voor de infrastructuur (IaaS) wordt breed een "pay-per-use" of "pay-as-you-grow" model aangeboden. Hierbij wordt afgerekend op basis van werkelijk verbruik van resources zoals vCPU, RAM en Storage (per GB).
- Managed Services (beheer) worden doorgaans verrekend op basis van een vast bedrag per eenheid, bijvoorbeeld per virtuele machine (VM) of per database-instantie per maand.
- Alle Deelnemers bieden de mogelijkheid voor maandelijkse rapportage en facturatie, waarbij inzicht wordt gegeven in het verbruik per onderdeel of per deelnemende organisatie van de Aanbestedende dienst.

Verschillen

- Deelnemer 2 en 4 maken een onderscheid tussen 'dedicated' resources en 'shared' resources; bij dedicated resources (zoals een eigen fysiek cluster) geldt vaak een vaste basisprijs ongeacht het verbruik, terwijl shared resources volledig variabel zijn.
- Deelnemer 7 en 9 bieden opties voor gereserveerde capaciteit (Reserved Instances), waarbij de Aanbestedende dienst korting krijgt in ruil voor een commitment op een minimale afname voor een langere periode.
- Sommige Deelnemers hanteren een prijsmodel dat inclusief alle licentiekosten is, terwijl andere Deelnemers ook 'Bring Your Own License' (BYOL) ondersteunen voor specifieke software.
- Deelnemer 3 geeft aan te werken met staffelprijzen: naarmate de afname van de totale Aanbestedende dienst stijgt, daalt de prijs per eenheid.

Conclusie
De markt is zeer flexibel in de verrekening en kan goed aansluiten bij de behoefte van de Aanbestedende dienst om kosten toe te wijzen aan de verschillende aangesloten organisaties. Het advies is om in de aanbesteding te vragen naar een transparante prijslijst voor de standaard bouwblokken (vCPU, RAM, GB), maar ook om een prijs te vragen voor de 'vaste' componenten die nodig zijn voor de gewenste mate van autonomie. Let hierbij specifiek op de impact van het nieuwe VMware-licentiemodel, aangezien dit de traditionele prijsopbouw per VM sterk kan beïnvloeden.

Analyse antwoorden op vraag 15
Hoe is de business continuïteit ingeregeld tijdens de migratie?

Overeenkomsten
- Alle Deelnemers benadrukken dat een gedetailleerd migratieplan per applicatie (runbook) de basis vormt voor continuïteit. Hierin worden de exacte stappen, afhankelijkheden en tijdlijnen vastgelegd.
- Er is consensus over het gebruik van bewezen replicatietechnologieën. Data wordt op de achtergrond gesynchroniseerd van de oude naar de nieuwe omgeving, waardoor de uiteindelijke 'overzetting' (cut-over) met minimale downtime kan plaatsvinden.
- Deelnemers hanteren standaard een "fallback" of "roll-back" scenario. Indien een migratie binnen het afgesproken tijdvenster niet succesvol blijkt, kan direct worden teruggekeerd naar de oorspronkelijke situatie in het oude datacenter.
- Migratiewerkzaamheden die impact hebben op de beschikbaarheid worden door alle Deelnemers gepland buiten kantoortijden of in specifieke onderhoudsvensters om de operationele verstoring voor de Aanbestedende dienst te minimaliseren.

Verschillen
- Deelnemer 3 en 8 stellen voor om eerst een 'pilot-migratie' of 'proefmigratie' uit te voeren met niet-kritische systemen om de methodiek en doorlooptijden te valideren voordat de vitale infrastructuur aan de beurt is.
- Deelnemer 1 en 5 leggen extra nadruk op de noodzaak van een tijdelijke dubbele infrastructuur ("dual-run"), waarbij systemen op beide locaties actief zijn totdat de volledige keten op de nieuwe locatie is geaccepteerd.
- Deelnemer 9 merkt op dat continuïteit ook afhangt van de netwerkverbindingen; zij adviseren redundante koppelingen tussen de oude en nieuwe omgeving gedurende de gehele migratieperiode om datapauzes te voorkomen.

- Enkele Deelnemers bieden aan om tijdens de migratie extra monitoring in te zetten op de oude omgeving, omdat daar vaak minder focus op ligt terwijl deze nog wel cruciaal is voor de business.

Conclusie
De markt beschouwt business continuïteit als een integraal onderdeel van hun migratiemethodiek. Voor de Aanbestedende dienst is het van belang om in de uitvraag te eisen dat de Deelnemer per migratie-wave een go/no-go moment inbouwt en een bewezen roll-back procedure kan overleggen. De grootste verantwoordelijkheid voor de Aanbestedende dienst ligt bij het tijdig testen en accepteren na een migratiestap, zodat de 'point of no return' pas wordt gepasseerd als de werking gegarandeerd is.

Analyse antwoorden op vraag 16
Hoe is de auditability ingeregeld?

Overeenkomsten
- Alle Deelnemers verklaren dat zij beschikken over de voor de overheid relevante certificeringen, zoals ISO 27001 (informatiebeveiliging), NEN 7510 (zorgspecifiek, indien van toepassing) en veelal ISAE 3402 Type II rapportages.
- Er is consensus dat de Aanbestedende dienst het recht behoudt om (periodieke) audits uit te voeren of te laten uitvoeren door een onafhankelijke derde partij (het "right to audit").
- Deelnemers bieden standaard uitgebreide logging en monitoring van alle beheerhandelingen op de infrastructuur (wie heeft wat, wanneer en waarom gedaan). Deze logs zijn onveranderbaar (tamperproof) opgeslagen.
- Alle Deelnemers geven aan dat zij periodiek rapportages opleveren over de afgesproken Service Level Agreements (SLA's) en de status van de beveiligingsmaatregelen.

Verschillen
- Deelnemer 5 en 8 onderscheiden zich door het aanbieden van een "continu auditing" dashboard, waarbij de Aanbestedende dienst realtime inzicht heeft in de naleving van specifieke BIO-controls (Basisbeveiligingsniveau Overheid).
- Deelnemer 1 en 4 verwijzen vaak naar hun wereldwijde compliance-portals waar de Aanbestedende dienst zelfstandig audit-rapporten en verklaringen kan downloaden, terwijl kleinere Deelnemers dit proces meer handmatig en op maat faciliteren.
- Deelnemer 9 biedt de mogelijkheid om "vulnerability scans" en penetratietesten direct te integreren in de audit-cyclus, waarbij de resultaten via een beveiligd portaal gedeeld worden.
- Enkele Deelnemers benadrukken dat zij de Aanbestedende dienst specifiek kunnen ondersteunen bij de eigen verantwoording richting toezichthouders door de technische bewijslast volledig aan te leveren.

Conclusie
De markt is goed voorbereid op de hoge audit-eisen van de Aanbestedende dienst. De focus verschuift van jaarlijkse "momentopnames" (zoals de ISAE 3402) naar meer continue vormen van aantoonbaarheid. Het advies aan de Aanbestedende dienst is om in de aanbesteding specifiek te vragen naar de aansluiting op de BIO (Baseline Informatiebeveiliging Overheid) en de wijze waarop de Deelnemer bewijslast aanlevert voor de jaarlijkse rechtmatigheidscontroles. Hiermee wordt voorkomen dat de audit-last alsnog zwaar op de eigen organisatie van de Aanbestedende dienst komt te rusten.

Analyse antwoorden op vraag 17
Hoe is het Service Level Management ingeregeld en hoe vindt de beheerinteractie plaats?

Overeenkomsten

- Deelnemers hanteren een structuur gebaseerd op ITIL-frameworks voor incident-, change- en problem-management.
- Voor de beheerinteractie bieden alle Deelnemers een centraal klantportaal aan voor het indienen en volgen van tickets, gecombineerd met een Service Desk voor telefonische en schriftelijke ondersteuning.
- Service Level Management wordt belegd bij een vaste Service Delivery Manager (SDM) die fungeert als het tactische aanspreekpunt voor de Aanbestedende dienst.
- Er vindt periodieke rapportage plaats (maandelijks of per kwartaal) over de gerealiseerde servicelevels, zoals beschikbaarheid, responstijden en de status van wijzigingen.
- De interactie is gelaagd: operationeel via de Service Desk, tactisch via de SDM en strategisch via een periodiek directieoverleg.

Verschillen

- Deelnemer 7 en 8 bieden een model van "Sovereign Operations", waarbij specifiek wordt gegarandeerd dat het beheer uitsluitend door in Nederland gescreend personeel wordt uitgevoerd, terwijl grotere Deelnemers (zoals 4 en 9) soms gebruikmaken van internationale 'Follow-the-Sun' supportcentra voor niet-gevoelige taken.
- Deelnemer 5 onderscheidt zich door een "Integrale Regie"-rol aan te bieden, waarbij zij ook de interactie met derde leveranciers van de Aanbestedende dienst coördineren (SIAM-model).
- Deelnemer 2 en 3 bieden meer flexibiliteit in de interactie door het gebruik van gedeelde communicatiekanalen zoals Slack of Microsoft Teams voor snelle, informele afstemming tussen beheerders.
- Enkele Deelnemers bieden een "Selfservice" portaal waarbij de Aanbestedende dienst zelf standaardwijzigingen (zoals het bijplaatsen van resources) kan doorvoeren zonder tussenkomst van een beheerder, wat de interactietijd verkort.

Conclusie
De markt biedt een volwassen en gestandaardiseerde aanpak voor Service Level Management. Voor de Aanbestedende dienst is het cruciaal om te bepalen hoeveel 'nabijheid' gewenst is. Waar de grotere Deelnemers uitblinken in gestandaardiseerde processen en portalen, bieden de kleinere Nederlandse Deelnemers vaak kortere lijnen en een persoonlijkere benadering. Het advies is om in de uitvraag specifiek te vragen naar de escalatiepaden en de talen waarin support wordt geboden (Nederlands vs. Engels), zeker gelet op de diverse achtergrond van de deelnemende gemeenten.

Analyse antwoorden op vraag 18
Zouden jullie de beschikbare selfservicefunctionaliteit kunnen beschrijven?

Overeenkomsten

- Vrijwel alle Deelnemers bieden een centraal Selfservice Portaal (vaak gebaseerd op technologieën zoals VMware Cloud Director, ServiceNow of een eigen ontwikkeld dashboard).
- Er is consensus dat standaard IaaS-taken door de Aanbestedende dienst zelf uitgevoerd kunnen worden, zoals het aanmaken, starten, stoppen en aanpassen (CPU/RAM) van virtuele machines.

- Beheer van opslag (provisioning van schijfruimte) en de basisconfiguratie van netwerkcomponenten (zoals firewalls, loadbalancers en VPN-tunnels) zijn nagenoeg altijd als selfservice beschikbaar.
- Alle portalen voorzien in Role-Based Access Control (RBAC), waardoor de Aanbestedende dienst per medewerker of per aangesloten gemeente specifieke rechten kan toekennen.

Verschillen

- Deelnemer 1 en 9 gaan een stap verder door ook PaaS-diensten (zoals 'Database-as-a-Service' of Kubernetes clusters) volledig via selfservice aan te bieden, terwijl andere Deelnemers dit nog via een service request (ticket) laten lopen.
- Deelnemer 5 en 7 leggen de focus op compliance-selfservice: zij bieden dashboards waarin de Aanbestedende dienst zelf realtime rapportages kan draaien over de status van de BIO-beveiligingsnormen.
- Deelnemer 4 en 8 bieden uitgebreide API-toegang, waardoor de Aanbestedende dienst de cloudfunctionaliteit direct kan koppelen aan eigen interne automatiseringstools (Infrastructure as Code).
- Sommige Deelnemers beperken selfservice tot technisch beheer, terwijl anderen ook financiële selfservice bieden, zoals het direct inzien van kosten per project of afdeling ('Showback' of 'Chargeback').

Conclusie

De markt is klaar voor een hoge mate van autonomie voor de Aanbestedende dienst. De keuze voor de Aanbestedende dienst is: willen we alleen technische knoppen om VM's te beheren, of zoeken we een portaal dat ook de administratieve en compliance-last (BIO-rapportages) verlicht? Het advies is om in de uitvraag te toetsen in hoeverre de selfservice-tooling intuïtief genoeg is voor de lokale beheerders van de gemeenten, zodat zij niet voor elke kleine wijziging afhankelijk zijn van de centrale Deelnemer.

Analyse antwoorden op vraag 19

In hoeverre is jullie organisatie in staat om specialismes te leveren qua beheer (database- en, netwerkbeheer)? En hoe denken jullie over het combineren van databasebeheer en eventueel netwerkbeheer bij 1 contractpartij?

Overeenkomsten

- Alle Deelnemers geven aan dat zij over gespecialiseerde teams beschikken voor zowel netwerkbeheer (LAN, WAN, Security) als databasebeheer (MS SQL, Oracle, PostgreSQL).
- Er is een unanieme voorkeur voor het beleggen van deze specialismes bij één contractpartij. Deelnemers stellen dat dit de complexiteit vermindert en de verantwoordelijkheid ("single point of accountability") verduidelijkt.
- Deelnemers zijn het erover eens dat de synergie tussen netwerk- en databasebeheer cruciaal is voor de performance en veiligheid van de keten. Door dit bij één Deelnemer onder te brengen, worden 'vingerwijzen' tussen verschillende betrokkenen bij incidenten voorkomen.
- Alle Deelnemers bieden deze diensten aan op basis van gestandaardiseerde beheerniveaus, variërend van enkel monitoring tot volledig "ontzorgd" functioneel en technisch beheer.

Verschillen

- Deelnemer 7 en 9 profileren zich specifiek op de bovenliggende applicatielaag en bieden ook diepgaande consultancy aan voor database-optimalisatie (tuning), terwijl anderen zich strikt beperken tot het operationeel houden van de database-engine.
- Deelnemer 5 en 8 benadrukken hun vermogen om netwerkbeheer naadloos te integreren met complexe security-eisen (zoals micro-segmentatie), wat volgens hen een directe meerwaarde biedt voor de autonomie en soevereiniteit van de Aanbestedende dienst.
- Enkele Deelnemers geven aan dat zij voor zeer specifieke legacy-databases (bijvoorbeeld oude Mainframe-omgevingen) mogelijk externe specialisten inhuren, terwijl de regie bij hen blijft liggen.

Conclusie
De markt is uitstekend in staat om deze specialismes integraal aan te bieden. Voor de Aanbestedende dienst biedt het combineren van netwerk- en databasebeheer bij één Deelnemer grote voordelen op het gebied van efficiëntie, snelheid van incidentoplossing en integrale beveiliging. Het advies is om in de uitvraag de grenzen van de verantwoordelijkheid scherp te trekken: waar stopt het databasebeheer van de Deelnemer en waar begint het applicatiebeheer van de Aanbestedende dienst

Analyse antwoorden op vraag 20
Hoe is fysieke toegang geregeld?
Overeenkomsten
- Deelnemers zijn zeer strikt in hun fysieke beveiligingsbeleid en maken gebruik van datacenters die minimaal Tier III gecertificeerd zijn en voldoen aan de ISO 27001 normering.
- Fysieke toegang is standaard beperkt tot een geautoriseerde groep medewerkers op basis van het "need-to-know" principe. Toegang wordt uitsluitend verleend na een strikte identiteitscontrole.
- Deelnemers zijn verantwoordelijk voor 24/7 camerabewaking (CCTV), inbraakdetectiesystemen en de aanwezigheid van fysieke beveiliging op de locaties waar de infrastructuur van de Aanbestedende dienst is ondergebracht.
- Er is consensus dat alle bezoekers (inclusief incidentele technici) zich moeten legitimeren en gedurende het gehele verblijf in het datacenter onder begeleiding staan van geautoriseerd personeel.
- Elke vorm van fysieke toegang wordt geregistreerd in een logboek dat voor auditdoeleinden beschikbaar is voor de Aanbestedende dienst.

Verschillen
- Deelnemer 5 en 7 bieden de optie voor fysiek gescheiden ruimtes (cages), waarbij de apparatuur van de Aanbestedende dienst achter een extra fysieke barrière wordt geplaatst die alleen toegankelijk is met een specifieke autorisatie.
- Deelnemer 4 en 9 maken gebruik van geavanceerde biometrische identificatie (zoals irisscans of vingerafdrukken) bij elke toegangssluis, terwijl andere Deelnemers vertrouwen op een combinatie van beveiligingspassen en visuele controle door beveiligingsbeambten.
- Sommige Deelnemers bieden de Aanbestedende dienst de mogelijkheid om zelf fysiek aanwezig te zijn bij specifieke hardware-interventies, terwijl anderen dit om veiligheidsredenen volledig in eigen beheer houden.
- Deelnemer 8 benadrukt dat hun datacenters specifiek gesitueerd zijn op Nederlands grondgebied om te voldoen aan de strengste soevereiniteitseisen, wat ook invloed heeft op wie er fysiek toegang krijgt tot het terrein.

Conclusie
De fysieke beveiliging is bij alle Deelnemers op een zeer hoog, marktconform niveau ingeregeld. De Aanbestedende dienst hoeft zich geen zorgen te maken over de basisbeveiliging. Indien de Aanbestedende dienst echter specifieke eisen heeft vanuit de BIO (bijvoorbeeld voor zeer vertrouwelijke data), is het raadzaam om in de uitvraag te vragen naar de mogelijkheden voor fysieke isolatie (cages) en de specifieke procedures rondom de vernietiging van defecte opslagmedia (data-dragers) op locatie.

Analyse antwoorden op vraag 21
Hoe zit het met interconnectiviteit met de buitenwereld?

Overeenkomsten
- Deelnemers zijn in staat om een breed scala aan connectiviteitsopties aan te bieden, variërend van publieke internetverbindingen tot hoogwaardige private koppelingen.
- Er is consensus dat voor de Aanbestedende dienst een hybride model het meest passend is: private verbindingen voor de koppeling tussen de eigen locaties en het datacenter, en beveiligde internet-breakouts voor publieke diensten.
- Deelnemers zijn aangesloten op de belangrijkste internetknooppunten (zoals AMS-IX) en bieden redundante verbindingen aan om de beschikbaarheid van de buitenwereld-connectie te garanderen.
- Alle Deelnemers ondersteunen het gebruik van VPN-technologieën (IPsec) en dedicated verbindingen (zoals Azure ExpressRoute of AWS Direct Connect) indien de Aanbestedende dienst ook gebruikmaakt van publieke cloud-aanbieders.
- Beveiliging van de buitenwereld-connectie wordt door alle Deelnemers geborgd middels Next-Generation Firewalls (NGFW) en DDoS-mitigatiediensten.

Verschillen
- Deelnemer 5 en 9 bieden de mogelijkheid voor een directe koppeling met landelijke netwerken zoals GGI-Net (Gemeentelijk Gemeenschappelijk Infrastructuur-Netwerk), wat voor de Aanbestedende dienst een pre kan zijn voor veilige communicatie met andere overheden.
- Deelnemer 4 en 1 benadrukken hun wereldwijde "backbone" netwerk, wat voordelen biedt bij het ontsluiten van diensten over grote geografische afstanden met zeer lage latentie.
- Deelnemer 8 onderscheidt zich door een sterke focus op soevereiniteit, waarbij zij garanderen dat al het netwerkverkeer binnen Nederlandse grenzen blijft ("local breakout"), tenzij expliciet anders gevraagd.
- Sommige Deelnemers bieden Software Defined Interconnect (SDI) aan, waarmee de Aanbestedende dienst via een portaal zelf real-time bandbreedte naar verschillende externe partijen kan opschalen of aanpassen

Conclusie
De technologische mogelijkheden voor interconnectiviteit zijn zeer uitgebreid. Het risico voor de Aanbestedende dienst ligt niet bij de beschikbaarheid van verbindingen, maar bij de complexiteit van de routering en de beveiliging van de verschillende verkeersstromen. Het advies is om in de aanbesteding specifiek te vragen naar de ondersteuning van **GGI-Net** en hoe de Deelnemer de transitie van de huidige netwerkverbindingen naar de nieuwe omgeving faciliteert zonder dat er "eilanden" in de communicatie ontstaan.

Analyse antwoorden op vraag 22

Welke virtualisatieplatformen bieden jullie aan?

Overeenkomsten

- Deelnemers zijn vrijwel allemaal aanbieders van VMware vSphere (ESXi) als primair platform. Dit wordt gezien als de standaard voor enterprise-omgevingen binnen de overheid vanwege de volwassenheid en de brede ondersteuning van applicatieleveranciers.
- Er is consensus dat de Aanbestedende dienst behoefte heeft aan een bewezen platform dat naadloos aansluit op de huidige on-premise omgevingen, om de migratie-effort (zonder herbouw van VM's) te minimaliseren.
- Deelnemers zijn in staat om naast traditionele virtualisatie ook container-virtualisatie (voornamelijk Kubernetes) aan te bieden voor modernere applicatielasten.
- Alle platformen die worden aangeboden, ondersteunen hoge beschikbaarheid (High Availability), automatische resource-verdeling (DRS) en live-migratie (vMotion).

Verschillen

- Deelnemer 5 en 8 bieden expliciet open-source alternatieven aan, zoals KVM of Proxmox, als reactie op de gewijzigde licentiestructuur en kostenstijgingen bij VMware. Zij positioneren dit als een manier om vendor lock-in te verminderen.
- Deelnemer 1 en 4 (de grotere cloudproviders) bieden hun eigen hypervisors aan die geoptimaliseerd zijn voor hun specifieke cloud-architectuur (bijv. Hyper-V gebaseerd of aangepaste KVM-varianten).
- Deelnemer 9 onderscheidt zich door een multi-hypervisor strategie aan te bieden, waarbij de Aanbestedende dienst binnen één portaal zowel VMware- als Nutanix AHV-omgevingen kan beheren.
- Sommige Deelnemers bieden enkel een 'managed' platform aan waarbij de Aanbestedende dienst geen toegang heeft tot de hypervisor-laag zelf, terwijl anderen meer vrijheid geven in de configuratie.

Conclusie

Hoewel VMware nog steeds de dominante standaard is onder de Deelnemers, is er door recente marktontwikkelingen een duidelijke trend zichtbaar naar alternatieve platformen. Het advies aan de Aanbestedende dienst is om in de uitvraag niet dwingend voor één specifiek merk (zoals VMware) te kiezen, maar functionele eisen te stellen aan het platform. Dit geeft Deelnemers de ruimte om met kostenefficiënte en toekomst vaste alternatieven te komen die passen binnen de begroting van de Aanbestedende dienst.

Analyse antwoorden op vraag 23

We hebben SOC/SIEM als dienst afgenomen bij een externe leverancier, hoe kunnen jullie hierop aansluiten?

Overeenkomsten

- Deelnemers zijn gewend om in een ecosysteem te werken waarbij security-monitoring door een derde partij (een extern Security Operations Center) wordt uitgevoerd.
- Er is consensus dat de basis van deze samenwerking ligt bij het ontsluiten van loggegevens. Deelnemers kunnen alle relevante logs van de infrastructuur (hypervisor, firewalls, netwerkapparatuur en opslag) doorsturen naar de SIEM-oplossing van de externe leverancier.
- Deelnemers zijn in staat om deze datastromen te faciliteren via standaardprotocollen (zoals Syslog, IPFIX of via API-koppelingen) over beveiligde verbindingen.

- Alle Deelnemers benadrukken dat er duidelijke werkafspraken moeten worden gemaakt over incidentrespons: wie krijgt welke melding en welke actie wordt er van de Deelnemer verwacht als het SOC een dreiging detecteert op de infrastructuur?

Verschillen

- Deelnemer 5 en 8 bieden aan om de koppeling te verrijken met vulnerability data uit de infrastructuur laag, zodat het SOC een completer beeld krijgt van de risico's.
- Deelnemer 4 en 9 kunnen ook 'agent-based' monitoring ondersteunen, waarbij zij toestaan dat de SOC-leverancier specifieke software (agents) installeert op de virtuele machines voor diepere inspectie (EDR/XDR).
- Sommige Deelnemers hanteren strikte scheidingslijnen en leveren enkel de ruwe data (logs), terwijl anderen bereid zijn om een actieve rol te spelen in het 'triage-proces' bij beveiligingsincidenten.
- Deelnemer 7 wijst erop dat zij de externe SOC-leverancier kunnen voorzien van een eigen 'read-only' dashboard in de cloudomgeving voor real-time inspectie tijdens een incident.

Conclusie

De integratie met een extern SOC/SIEM is technisch goed te realiseren en is een veelvoorkomend scenario. Voor de Aanbestedende dienst ligt de uitdaging vooral op het procesmatige vlak: de interactie tussen de cloudleverancier en de SOC-leverancier. Het advies is om in de aanbesteding een Dossier Afspraken en Procedures (DAP) te eisen waarin de ketenverantwoordelijkheid bij beveiligingsincidenten exact wordt vastgelegd. Hiermee wordt voorkomen dat er kostbare tijd verloren gaat bij een daadwerkelijke cyberdreiging.

Analyse antwoorden op vraag 24

Dienen wij als organisatie zelf zorg te dragen voor aanschaf en beheer van de licenties, of is dat onderdeel van de geleverde dienst?

Overeenkomsten

- Deelnemers zijn in staat om beide modellen te ondersteunen: het leveren van licenties als onderdeel van de dienst (managed licenties) of het faciliteren van door de Aanbestedende dienst zelf ingebrachte licenties (Bring Your Own License - BYOL).
- Er is consensus dat de infrastructuur-gebonden licenties (zoals VMware/virtualisatie en Windows Server via het SPLA-model) doorgaans het meest efficiënt door de Deelnemer geleverd kunnen worden. Dit ontzorgt de Aanbestedende dienst op het gebied van compliance en rapportage.
- Deelnemers zijn verantwoordelijk voor de monitoring en rapportage van de licenties die zij zelf leveren, waarbij de Aanbestedende dienst maandelijks betaalt op basis van het werkelijke gebruik.
- Voor applicatie-specifieke licenties (zoals Oracle, SAP of specifieke gemeentelijke software) adviseren bijna alle Deelnemers dat de Aanbestedende dienst deze zelf blijft beheren, aangezien de contractuele relatie met de softwareleverancier vaak al lokaal is vastgelegd.

Verschillen

- Deelnemer 1 en 4 bieden uitgebreide portals voor Software Asset Management (SAM), waarmee de Aanbestedende dienst ook inzicht krijgt in de compliance van de zelf meegebrachte licenties.
- Deelnemer 5 en 7 wijzen op de recente strategische koerswijzigingen van partijen als Broadcom (VMware), waarbij zij adviseren om de licenties voor het virtualisatieplatform juist

integraal onderdeel te maken van de dienst om prijsrisico's en beheerlast bij de Aanbestedende dienst weg te nemen.
- Deelnemer 8 en 9 maken een onderscheid in het beheer: zij kunnen het technisch beheer (installatie en updates) van licenties overnemen, ook als de Aanbestedende dienst de juridische eigenaar van de licenties blijft.
- Sommige Deelnemers bieden de mogelijkheid om licenties van de Aanbestedende dienst over te nemen in hun eigen contracten (novatie), om zo schaalvoordeel te behalen.

Conclusie
De markt biedt volledige flexibiliteit. Het meest voorkomende advies is een hybride model: de Deelnemer levert de licenties voor de infrastructuur en het besturingssysteem (Windows Server/Linux), terwijl de Aanbestedende dienst eigenaar blijft van de functionele applicatielicenties. Dit model biedt de beste balans tussen ontzorging en behoud van regie op de eigen software-omgeving. Het is raadzaam om in de aanbesteding specifiek te vragen naar hoe de Deelnemer omgaat met licentie-audits en het bewijzen van compliance voor de BYOL-onderdelen.

Analyse antwoorden op vraag 25
Wat adviseren jullie omtrent bring your own key en data-encryptie?

Overeenkomsten
- Deelnemers zijn unaniem van mening dat data-at-rest (opgeslagen data) en data-in-transit (data over het netwerk) standaard versleuteld moeten zijn om te voldoen aan de BIO-normen.
- Er is consensus dat encryptie op infrastructuurniveau door de deelnemer wordt beheerd (provider-managed encryption), waarbij de deelnemer zorg draagt voor het sleutelbeheer voor de algemene opslagomgeving.
- Deelnemers zijn in staat om Bring Your Own Key (BYOK) te ondersteunen, waarbij de Aanbestedende dienst de controle behoudt over de eigen cryptografische sleutels via een Key Management System (KMS).
- Alle partijen benadrukken dat het gebruik van BYOK een hogere mate van verantwoordelijkheid bij de Aanbestedende dienst legt (als de eigen sleutel verloren gaat, is de data onherstelbaar verloren voor beide partijen).

Verschillen
- Deelnemer 4 en 9 bieden geavanceerde Hardware Security Modules (HSM) in de cloud aan waarmee de Aanbestedende dienst sleutels kan genereren die zelfs voor de cloudprovider technisch ontoegankelijk zijn.
- Deelnemer 5 en 8 adviseren om BYOK alleen in te zetten voor zeer gevoelige data (Hoge Beschikbaarheid/Vertrouwelijkheid), omdat de complexiteit en de kans op menselijke fouten bij het beheer van eigen sleutels aanzienlijk is.
- Sommige Deelnemers bieden een tussenoplossing genaamd Hold Your Own Key (HYOK), waarbij de sleutel fysiek op de locatie van de Aanbestedende dienst blijft staan en nooit de cloudinfrastructuur betreedt.
- Deelnemer 7 onderscheidt zich door een beheerde KMS-dienst aan te bieden waarbij zij de Aanbestedende dienst adviseren en ondersteunen bij de levenscyclus van de sleutels (genereren, roteren en vernietigen).

Conclusie
De markt adviseert om encryptie standaard in te regelen op basis van provider-managed keys voor reguliere workloads, vanwege de balans tussen veiligheid en beheerbaarheid. Voor specifieke

applicaties met een zeer hoog risicoprofiel is BYOK een geschikte oplossing. Het advies aan de Aanbestedende dienst is om in de uitvraag te eisen dat de Deelnemer een robuust Key Management beleid heeft dat voldoet aan de BIO, en om per type data te bepalen of de extra complexiteit van BYOK opweegt tegen het verlaagde risico op ongeautoriseerde toegang door de beheerder.

Analyse antwoorden op vraag 26
Welke flexibiliteit hebben we indien we patchmanagement m.b.t. OS afnemen, denk bijv. aan service windows?

Overeenkomsten

- Deelnemers zijn in staat om het patchmanagement volledig over te nemen voor standaard besturingssystemen zoals Windows Server en diverse Linux-distributies.
- Er is consensus dat patching plaatsvindt binnen vooraf overeengekomen service windows (onderhoudsvensters) om de impact op de bedrijfsvoering te minimaliseren.
- Deelnemers zijn gewend te werken met een gelaagd patchmodel, waarbij patches eerst in een test- of acceptatieomgeving worden uitgerold voordat de productieomgeving aan de beurt is (OTAP-strategie).
- Alle Deelnemers bieden de mogelijkheid om kritieke security patches met spoed buiten de reguliere vensters om te installeren indien de ernst van de dreiging dit vereist, uiteraard in nauw overleg met de Aanbestedende dienst.

Verschillen

- Deelnemer 2 en 5 bieden volledige flexibiliteit waarbij de Aanbestedende dienst per applicatie of per servergroep specifieke tijdsloten kan definiëren in een selfservice portaal.
- Deelnemer 4 en 9 maken gebruik van verregaande automatisering waarbij patches continu klaarstaan en de Aanbestedende dienst via een druk op de knop ("on-demand") de herstart van de servers kan initiëren na de patchronde.
- Sommige Deelnemers hanteren vaste standaardvensters (bijvoorbeeld de tweede dinsdag of woensdag van de maand) en brengen extra kosten in rekening voor afwijkende of klantspecifieke tijdstippen.
- Deelnemer 8 onderscheidt zich door een "zero-downtime" patching benadering aan te bieden voor specifieke clusters, waarbij servers om de beurt worden gepatcht zodat de dienstverlening altijd beschikbaar blijft.

Conclusie
De markt biedt voldoende flexibiliteit om aan te sluiten bij de diverse onderhoudsbehoeften van gemeenten. De belangrijkste afweging voor de Aanbestedende dienst is de balans tussen maatwerk en kosten; hoe specifieker het service window per server, hoe hoger de beheerlast. Het advies is om in de uitvraag te vragen naar de mogelijkheid om verschillende "onderhoudsprofielen" te definiëren (bijvoorbeeld: kantoortijden, weekenden of nachtelijke uren), zodat de kritische applicaties van de gemeenten altijd op het meest gunstige moment worden bijgewerkt.

Analyse antwoorden op vraag 27
De RID wil een autonoom (volledig gescheiden) compartiment. Op welke manier kunnen jullie dit garanderen, welke opties zijn er en welke impact hebben de verschillende opties op de kosten?

Overeenkomsten

- Alle Deelnemers maken een onderscheid tussen drie hoofdvormen van isolatie: logische isolatie, dedicated clusters en volledige fysieke isolatie.
- Er is consensus dat logische isolatie (softwarematig) de meest kostenefficiënte en flexibele optie is.
- Volledige fysieke isolatie (eigen hardware in eigen racks) wordt door iedereen als de duurste optie met de minste schaalbaarheid omschreven.

Verschillen

- Deelnemer 3 adviseert expliciet om de behoefte functioneel uit te vragen in plaats van technisch, om leveranciers de ruimte te geven voor de beste technische invulling.
- Deelnemer 6 geeft aan altijd gebruik te maken van gedeelde centrale netwerk- en storage-resources, maar wel dedicated servers aan te kunnen bieden.
- Deelnemer 2 benadrukt dat volledige fysieke scheiding ook significante impact heeft op beheer- en auditmaatregelen.

Conclusie

Hoewel fysieke autonomie mogelijk is, waarschuwen de Deelnemers unaniem voor de hoge kosten en beperkte flexibiliteit. Logische isolatie met dedicated componenten lijkt de meest aanbevolen balans tussen veiligheid en budget.

3 Eindconclusie van de Marktconsultatie

Op basis van de resultaten van de Marktconsultatie kan worden geconcludeerd dat de markt voor managed private cloud diensten zeer volwassen is en voldoende gekwalificeerde Deelnemers biedt om de ambities van de Aanbestedende dienst te realiseren. De Marktconsultatie bevestigt dat de Deelnemers de gestelde deadline voor de datacenter-exit per 1 juli 2027 als haalbaar beschouwen, mits de uitvoering uiterlijk in het eerste kwartaal van 2026 start.

Een hybride cloud-strategie wordt door de markt breed ondersteund als de meest duurzame keuze, waarbij de private cloud essentieel blijft voor het borgen van soevereiniteit en het voldoen aan strikte wet- en regelgeving zoals de BIO en NIS2. Hoewel technische autonomie en fysieke isolatie van hardware mogelijk zijn, waarschuwen de deelnemers unaniem voor de hoge kosten en de beperkte flexibiliteit die dit met zich meebrengt. Een model gebaseerd op logische isolatie met dedicated componenten lijkt de meest optimale balans tussen veiligheid en budget. Op het gebied van beheer en techniek laten de reacties zien dat deelnemers goed in staat zijn om de regie te voeren over complexe ketens, inclusief gespecialiseerd netwerk- en databasebeheer en de integratie met externe securitydienstverleners (SOC/SIEM). Er is een duidelijke verschuiving zichtbaar van traditionele licentiemodellen naar flexibele, gebruik-gebaseerde kostenstructuren, waarbij de markt adviseert om infrastructuur-gebonden licenties integraal onderdeel te maken van de dienstverlening.

De uiteindelijke conclusie is dat de Aanbestedende dienst een realistische opdracht in de markt zet. Het succes van de aanbesteding en de migratie hangt echter sterk af van de interne voorbereiding. Een actuele en volledige inventarisatie van het IT-landschap en een sterke centrale regie-organisatie zijn randvoorwaarden om de innovatiekracht van de markt optimaal te benutten en de continuïteit van de dienstverlening aan de aangesloten gemeenten te waarborgen.

Let op:
Een additionele informatiebijeenkomst met Deelnemers is niet benodigd.